UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/718,041	11/20/2000	Charles A. Kunzinger	RSW920000100US1	2219

7590 07/27/2004

Gerald R Woods
IBM Corporation
T81/503
P O Box 12195
Research Triangle Park, NC 27709

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/718,041	KUNZINGER, CHARLES A.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- Th MAILING DATE of this communication appears on the cov r sheet with th corr spondenc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-36 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-36 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 20 November 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 11/20/2000.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-36 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 32 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claim 32 recites the limitation "the boundary device" in line 2; however, the limitation fails to particularly point out which of the two distinct boundary devices defined in parent claim 28 contain the security enforcement functions.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claim 36 is rejected under 35 U.S.C. 102(b) as being anticipated by Boyle U.S. Patent No. 5,940,591 (hereinafter Boyle).

7. As per claim 36, Boyle discloses a method for providing fine-grained, identity-based access control in a computer networking environment (see Boyle, Figure 1), comprising steps of:

a. establishing a mutually-authenticated connection between a first device and a second device using strong cryptographic techniques (see Boyle, col. 10, line 26-col. 11, line 18);

b. extracting a first authenticated identity associated with the first device and a second authenticated identity associated with the second host during the step of establishing the mutually-authenticated connection (see Boyle, col. 10, lines 27-31; col. 11, lines 2-10);

c. providing secure communications between a security enforcement function and an access control function (see Boyle, col. 8, lines 45-47 and 50; Figure 5A, 6A and 6B);

d. providing the extracted first and second authenticated identities, by the security enforcement function, to the access control function (see Boyle, Figure 4C; col. 7, lines 55-58; col. 10, lines 31-33; col. 11, lines 9-10; claim 2);

e. determining access privileges of the first device and the second device, by the access control function, based upon the provided extracted identities (see Boyle, col. 10, lines 33-36 and 42; col. 11, lines 11-14; claim 2); and

f. securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined

access privileges (see Boyle, col. 3, lines 31-36; col. 10, lines 40-65, especially line 42; col. 11, lines 14-18).

The aforementioned covers claim 36.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings, Cryptography and Network Security (hereinafter Stallings) in view of Boyle.

10. As per claims 1 and 5, Stallings discloses a computer network security apparatus for providing coarse-grained access control in a computer networking environment, the apparatus embodied on one or more computer-readable media and comprising:

a. computer-readable program code means for establishing a first security association between a first host and a boundary device, wherein the first security association uses strong cryptographic techniques (see Stallings, page 411, Figure 13.5, 'End-to-intermediate authentication'; page 404-407, 'Security Associations', especially first paragraph in section; page 420, Figure 13.10, Reference No. (d) Case 4);

b. computer-readable program code means for establishing a second security association between a second host and the boundary device, wherein the second security association uses strong cryptographic techniques (see Stallings, page 411, Figure 13.5, 'End-to-intermediate authentication'; page 404-407, 'Security Associations', especially first paragraph in section; page 420, Figure 13.10, Reference No. (d) Case 4);

c. computer-readable program code means for extracting, by a security enforcement function in the boundary device, a first authenticated identity associated with the first host during operation of the computer-readable program code means for establishing the first security association (see Stallings, page 412, Figure 13.6 and first paragraph, 3rd full sentence);

d. computer-readable program code means for extracting, by the security enforcement function in the boundary device, a second authenticated identity association with the second host during operation of the computer-readable program means for establishing the second security association (see Stallings, page 412, Figure 13.6 and first paragraph, 3rd full sentence);

e. computer-readable program code means for providing the extracted first authenticated identity and the extracted second authenticated identity, by the security enforcement function to an access control function (see Stallings, page 412, Figure 13.6 and first paragraph, 3rd full sentence);

f. computer-readable program code means for determining access privileges of the first host and the second host, by the access control function, based upon

the provided extracted identities (see Stallings, page 404, Table 13.1, 'Access Control'; page 412, first paragraph, 3rd full sentence).

11. Stallings does not expressly disclose the security enforcement function and the access control function as being in separate devices and hence requiring a secure channel between the two functions. Boyle teaches a network security configuration wherein a secure channel is established between a security enforcement function contained in a boundary device and an access control function contained in a security manager (see Boyle, Figure 2; col. 7, lines 55-58; col. 8, lines 39-51, especially lines 45-47 and 50; claim 2). It would be obvious to one of ordinary skill in the art at the time the invention was made for the security enforcement function to be situated in a boundary device and the access control function to be situated in a security manager wherein communications between the two functions are secured as taught by Boyle since this configuration enables administrative policies to be centralized in a single unit, modularizes the devices of the architecture by dividing labor into their respective devices, and secures distribution of administrative directives in a secure channel (see Boyle, Figure 2; col. 2, lines 59-62).

12. Finally, the network security configuration disclosed by Boyle implements a fine-grained, identity-based access control methodology administered by the security manager, wherein the authenticated identities are used to determine access privileges of the hosts (see Boyle, col. 5, lines 29-60; Figure 6A; claim 2). It would be obvious to one of ordinary skill in the art at the time the invention was made for the access controls to be based on the identities of the communicating entities since doing so restricts

access based on user-defined attributes (see Boyle, col. 1, lines 44-46). The aforementioned cover claims 1 and 5.

13. As per claim 2, Stallings covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 102(b). In addition, the strong cryptographic techniques used for the first security association and second security association are provided by protocols known as IKE and IPsec (see pages 402-408, section 13.2, 'IP Security Architecture' and pages 421-431, section 13.6, 'Key Management').

14. As per claim 3, Stallings covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Stallings and Boyle disclose the apparatus further comprises:

a. computer-readable program code means for securely making the determined access privileges available to the security enforcement function (see Boyle, col. 8, lines 45-47); and

b. computer-readable program code means for using the made-available access privileges to determine whether to forward a packet flowing between the first host and the second host or to discard the packet (see Stallings, page 404, Table 13.1, 'Access control'; page 412, Figure 13.6 and 1st paragraph, 3rd full sentence).

15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the access privileges to be securely made available to the security

enforcement function wherein the access privileges determine whether or not to forward a packet flowing between the first host and the second host since these means enable secure administration of access control on a packet level (see Stallings, page 400, 3rd full paragraph; page 401, Figure 13.1). The aforementioned covers claim 3.

16. As per claim 4, Boyle covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Stallings and Boyle disclose the apparatus further comprises:

a. computer-readable program code means for securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined access privileges (see Boyle, col. 8, lines 45-47; col. 10, line 42); and

b. computer-readable program code means for using the communicated packet-handling directives to determine whether or not to forward a packet flowing between the first host and the second host or to discard the packet (see Stallings, page 404, Table 13.1, 'Access control'; page 412, Figure 13.6 and 1st paragraph, 3rd full sentence).

17. It would be obvious to one of ordinary skill in the art at the time the invention was made for packet-handling directives from the access control function to be securely communicated to the security enforcement function wherein the packet-handling directives determine whether or not to forward a packet flowing between the first host and the second host since these means enable access directives to be generated in a

centralized device-within the security manager (see Boyle, col. 8, lines 47-51). The aforementioned covers claim 4.

18. As per claims 6 and 9, Stallings covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the security associations defined by Stallings specify only coarse-grained access control information (see Stallings, pages 402-408, section 13.2 'IP Security Architecture'; see applicant's specification page 7, 2nd paragraph, 2nd sentence for basis of "coarse-grained" access control use in IPsec). The aforementioned cover claims 6 and 9.

19. As per claims 7, 8, 10 and 11, Stallings covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the authenticated identities associated with the hosts are an identification of a user or an application on the hosts (see Stallings, page 401, Figure 13.1). The aforementioned cover claims 7, 8, 10 and 11.

20. As per claims 12-16, 18 and 19, they are system claims corresponding to claims 1-11 and they do not teach or define above the information claimed in claims 1-11. Therefore, claims 12-16, 18 and 19 are rejected as being unpatentable over Stallings in view of Boyle for the same reasons set forth in the rejections of claims 1-11.

21. As per claim 17, Stallings covers a system as outlined above in the claim 5 and 12 rejections under 35 U.S.C. 103(a). In addition, the security enforcement functions are located in the first and second hosts (see Stallings, page 401, Figure 13.1, 'User system with IPSec').

22. As per claims 20-27, they are method claims corresponding to claims 12-19 and they do not teach or define above the information claimed in claims 12-19. Therefore, claims 20-27 are rejected as being unpatentable over Stallings in view of Boyle for the same reasons set forth in the rejections of claims 12-19.

23. As per claim 28, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Stallings discloses a first security association between a first host and a first boundary device and a second security association between a second host and a second boundary device (see Stallings, page 420, Figure 13.10, Reference No. (c) Case 3).

24. As per claims 29-35, they are method claims corresponding to claims 20-28 and they do not teach or define above the information claimed in claims 20-28. Therefore, claims 29-35 are rejected as being unpatentable over Stallings in view of Boyle for the same reasons set forth in the rejections of claims 20-28.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Holden et al. U.S. Patent No. 5,802,178.

Holden et al. U.S. Patent No. 6,067,620.

Williams U.S. Patent No. 6,304,973 B1.

Rothermel et al. U.S. Patent No. 6,678,827.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
July 19, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER